

### **REMARKS/ARGUMENTS**

This Amendment is in response to the Office Action mailed on October 18, 2005 ("Office Action"). Claims 1-36 were rejected. Review and reconsideration are requested in view of the following remarks. Additionally, Applicants have amended claims 1, 25, 35 and 36, and have added new claims 37-43.

#### **Examiner Interview**

Applicants thank the Examiner for the courtesy extended to the Applicants' representative in granting a telephonic interview, which took place April 13, 2006. Applicants' representative explained that the invention is not anticipated or rendered obvious by the reference Campbell and Orchier. It was explained that the references fail to teach the event parser in communication with multiple network service devices. It was discussed that the Campbell reference fails to teach such an approach and is directed to monitoring of hosts. Claim 25 was discussed, which has language regarding a firewall, VPN server or router and e-mail server.

It was pointed out that claim 1 teaches an event broadcaster being able to transmit event objects in real time, while in contrast Campbell teaches shared data structures and transmitting a warning message. It was explained that Campbell does not teach the claimed transmission of event objects in real time, as an intrusion alarm as claimed in claim 1.

Applicants explained that the claims would be allowable over the cited references without amendment. However, in order to expedite processing of claims to allowance, Applicants indicated that an amendment may be submitted.

#### **Amendment of Claims 1, 25, 35 and 36 under 35 U.S.C. § 102(e); New Claims 37-43**

It is believed that the claims would be allowable over the cited references without amendment for the reasons set forth below. However, in order to expedite processing of claims to allowance, Applicants have made certain amendments to the claims without prejudice as set forth above. Applicants reserve the right to pursue the claims in their unamended form in a continuation application.

New claims 37-43 have been added in order to more fully claim embodiments of Applicants' invention. Review and approval are respectfully requested.

**Rejection of Claims 1, 25, 35 and 36 under 35 U.S.C. § 102(e)**

Claims 1, 25, 35 and 36 were rejected under 35 U.S.C. § 102(e) as being anticipated by US Patent No. 6,839,850 (Campbell). Applicants respectfully traverse the rejection.

The Office Action argues that Campbell teaches the claimed event parser in communication with multiple network service devices, pointing to Campbell, column 5, lines 35-41 and column 12, lines 58-67. Such column 5, lines 35-41 teaches a SI&W engine usable in conjunction with audit agents. However, there is no teaching of the claimed event parser in communication with multiple network service devices. Campbell discloses "network devices," for example as follows:

FIG. 1 is a block diagram illustrating an exemplary computer network 100 including a plurality of network devices on which an embodiment of the invention can be used. The network devices include devices such as hosts, servers, workstations, and personal computers (PCs). The present invention is usable on such networks as ARCnet, Ethernets and Token-Ring networks, wireless networks, among other networks. The network 100, in this example, has a central network cable 102, also known as media, which may be of any known physical configuration including unshielded twisted pair (UTP) wire, coaxial cable, shielded twisted pair wire, fiber optic cable, and the like. Alternatively, the network devices could communicate across wireless links.

Campbell, column 7, line 65 - column 8, line 11 (emphasis added). As shown above, in Campbell "The network devices include devices such as hosts, servers, workstations, and personal computers (PCs)." Thus, Campbell fails to teach the claimed event parser in communication with multiple network service devices.

Additionally, regarding claim 1, the Office Action argues that Campbell teaches an event broadcaster being able to transmit event objects in real time, relative to the receipt of the log data, as an intrusion alarm. It is believed that Campbell does not teach the claimed approach. Campbell does teach shared data structures. Campbell also teaches causing a warning message to be displayed when a warning is produced by the analysis functions. See for example, Campbell, column 12, line 47-53. However, such teaching does not teach or suggest the

claimed approach of an event broadcaster being able to transmit event objects in real time, relative to the receipt of the log data, as an intrusion alarm.

Weight must be given to all the elements of the claim. See MPEP 2131 (regarding Anticipation -- Application of 35 USC 102(a), (b), and (e), subsection entitled "To Anticipate a Claim, the Reference Must Teach Every Element of the Claim"), which states:

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.

(Emphasis added.) As shown above, elements of claim 1 are not found in Campbell. Thus, for the reasons discussed above, it is believed that anticipation of claim 1 has not been established and that the rejection should be removed.

Claims 25, 35 and 36 were rejected under 35 U.S.C. § 102(e) based on similar reasoning as to claim 1. It is therefore believed that the rejection of such claims has also been overcome.

**Rejection of Claims 1-10, 12-15, 17-22, 25-31, 33 and 34 under 35 U.S.C. § 103(a)**

Claims 1-10, 12-15, 17-22, 25-31, 33 and 34 were rejected under 35 U.S.C. § 103(a) as being unpatentable over prior art of record, US Patent No. 6,070,244 (Orchier) and further in view of Campbell. Applicants respectfully traverse the rejection.

The Office Action recognizes that Orchier fails to teach transmitting the claimed event object in real time, relative to receipt of the claimed log data, as an intrusion alarm. However, the Office Action looks to Campbell for this deficiency arguing that it would be obvious to combine Campbell with Orchier. Applicants disagree.

Campbell does not teach the claimed approach of transmitting the claimed event object in real time, relative to receipt of the claimed log data, as an intrusion alarm. As discussed above, Campbell does teach shared data structures, and Campbell also teaches causing a warning message to be displayed when a warning is produced by the analysis functions. See for example, Campbell, column 12, line 47-53. However, such teaching does not teach or suggest the claimed approach of an event broadcaster being able to transmit event objects in real time, relative to the receipt of the log data, as an intrusion alarm.

Thus, even in combination, the references fail to teach or suggest the invention as claimed in claim 1. Therefore, it is believed that *prima facie* obviousness has not been established regarding claim 1 in view of the cited references. See MPEP 2143.03:

To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art.

(emphasis added). As shown above, not all the limitations are taught or suggested by the cited references, even in combination. Therefore, it is believed that the rejection should be removed.

Additionally, it is believed that one of ordinary skill in the art would not be motivated to modify Orchier to transmit the claimed event object in real time, relative to receipt of the claimed log data, as an intrusion alarm. Rather, Orchier teaches away from such a modification in view of Campbell. See MPEP 2141.02:

A prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention.

(emphasis added). Orchier teaches a batch approach with actions at scheduled intervals. See for example, Figures 4b, 4c, and 4e of Orchier, which refer to actions taking place at a designated time of day. Thus, Orchier is teaching a batch approach, rather than a real time approach. See also Orchier, column 11, lines 4-6, which refer to steps including scheduling the starting of the program at a designated time of day. Thus, one skilled in the art would not be motivated to modify Orchier in order to transmit the claimed event object in real time, relative to receipt of the claimed log data, as an intrusion alarm, since such a goal is contrary to the teaching of Orchier. See MPEP 2143.01:

If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious.

(emphasis added). Therefore, for this additional reason Orchier and Campbell fail to render the invention of claim 1 obvious and it is believed that the rejection of claim 1 should be removed. Accordingly, removal of the rejection of claim 1 is respectfully requested.

Claim 1 also refers to intrusion events from log data received from network services devices in a computer network. Orchier does not provide teaching or suggestion of handling of network intrusion events from log data received from network services devices as claimed in claim 1. For this additional reason, it is believed that the rejection of claim 1 should be removed.

Claims 25, 35 and 36 were rejected under 35 U.S.C. § 103(a) based on similar reasoning as to claim 1. It is therefore believed that the rejection of such claims has also been overcome.

### **Rejection of Dependent Claims**

The rejections of dependent claims in the present application are believed overcome based at least for the reasons as to their parent claims, as discussed above. Additionally, it is believed that such claims are independently patentable. Applicants have also presented reasons for patentability of such claims in a previous response, and Applicants incorporate such reasons herein by reference. It is believed that the Office Action has not addressed Applicants' arguments as to patentability of such claims.

For example, with respect to claims 7 and 30, the Office Action cites Orchier, column 13, lines 45-50 and Fig. 8b, "Note" for teaching a report console further configured to display query result data and summary lines, said summary lines comprising hypertext links providing access to further data. Office Action at page 11 (emphasis added). The cited text of Orchier does not appear to teach such an approach including hypertext links providing access to further data. Rather, such portion of Orchier provides:

[Both] standard and ad-hoc queries are supported by the software implementation of the agent 82. The query agent 82 has been reduced to practice in a form that uses an Internet/Intranet technology, i.e. a web browser, to allow access with a minimum of connectivity and software distribution problems. Any query tools that handles Sybase™ could be used [in the implementation.]

Orchier, column 13, lines 45-50. The use of Internet/Intranet technology, i.e., a web browser, as disclosed in Orchier fails to teach the particular use of summary lines comprising hypertext links providing access to further data. Such teaching of such a particular approach is not present in the general discussion of Internet/Intranet technology or a web browser. Thus, it is believed the rejection with respect to claims 7 and 30 should be removed, and such action is respectfully requested. The current Office Action has not addressed Applicants' arguments in this regard.

Claim 9 was rejected citing column 2, lines 30-35 Orchier for teaching a graphical user interface displaying the status of network security devices in real time. Office Action at 11. It is believed that such interpretation of Orchier is incorrect. The cited portion of Orchier, provides:

The technology independent layer handles the main functionality of the system: locating terminating employees, auditing system and user data, monitoring security events (e.g. failed login attempts), automatically initiating corrective action, interfacing with the system users, reporting, querying and storing of collected data.

Orchier, column 2, lines 30-35. Such description fails to teach a graphical user interface displaying the status of network security devices in real time. In fact, the cited portion of Orchier is directed to a layer of a layered software architecture. The cited portion is related to a technology independent layer of the software. This general discussion fails to teach a graphical user interface to explain the status of network security devices in real time. The current Office Action has not addressed Applicants' arguments in this regard.

Claims 12, 33 and 34 were rejected based on a citation of Orchier, column 13, lines 10-15 and column 14, lines 5-10, for a teaching of a chat manager accessible to a user from an alarm console for executing electronic communications links between the user and others having an electronic communication link to the computer system. Office Action at 12. The cited description of Orchier fails to teach a chat manager. The cited portion of Orchier provides:

... of certain key security or operating system files within any one of the security domains 70a-70n. The alert agent 80 automatically notifies appropriate personnel by e-mail, phone and/or pager. This is indicated by the alarm arrow 81 in Fig. 3b. The alert agent 80 is unique in that it is able to monitor across dissimilar environments, ...

Orchier, column 13, lines 10-15. Applicants fail to find any teaching of the chat manager. A chat manager does not follow from teaching of notification by email, phone and/or pager. Therefore, it is believed that the rejection of claims 12, 33 and 34 is in error and should be removed. Such action is respectfully requested. The current Office Action has not addressed Applicants' arguments in this regard.

Thus, for the reasons set forth above, it is believed that the rejection of the dependent claims in the application should also be removed.

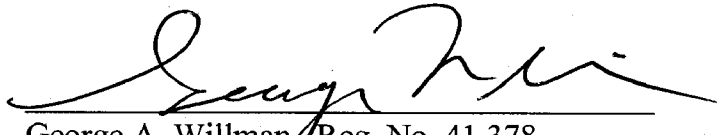
**CONCLUSION**

Applicants submit that the instant application is in condition for allowance. Should the Examiner have any questions, the Examiner is requested to contact the undersigned attorney.

The Commissioner is authorized to charge any additional fees which may be required, including petition fees and extension of time fees, to Deposit Account No. 23-2415 (Docket No. 26836.701.201).

Respectfully submitted,  
WILSON SONSINI GOODRICH & ROSATI

Date: April 17, 2006

  
George A. Willman, Reg. No. 41,378

650 Page Mill Road  
Palo Alto, CA 94304  
(650) 493-9300  
**Customer No. 021971**